PUBLIC KEY INFRASTRUCTURE

IMPLEMENTATION PLAN

FOR THE DEPARTMENT OF THE NAVY

29 November 2000

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 29112000	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle Public Key Infrastructure Implementation Plan for the Department of the Navy	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Department of the Navy	**Performing Organization Number(s)**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms "IATAC COLLECTION"	
Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 21	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	11/29/00	Report

4. TITLE AND SUBTITLE
Public Key Infrastructure Implementation Plan for the Department of the Navy

5. FUNDING NUMBERS

6. AUTHOR(S)

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

This PKI Implementation Plan for the Department of the Navy (DON) provides a roadmap for Navy and Marine Corps planners and managers to carry out the DoD PKI policy and addresses the general activities and objectives associated with implementation of the Navy and Marine Corps portions of the Class 3, Class 4 (FORTEZZA), and Target Class 4 DoD PKIs. This implementation plan is consistent with the 6 May 1999 "DoD Public Key Infrastructure" memorandum released by the Deputy Secretary of Defense, as modified by the DoD Chief Information Officer (CIO) on 12 August 2000, as well as the 29 October 1999 DoD PKI Implementation Plan. Chief of Naval Operations (CNO) N643 and Headquarters, Marine Corps (HQMC) C4 will promulgate detailed implementation guidance within their respective chains-of-command as necessary to accomplish the specific activities and achieve the specific objectives outlined in this plan.

14. SUBJECT TERMS	15. NUMBER OF PAGES
PKI	
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	UNCLASSIFIED	UNCLASSIFIED	None

Foreword

The 6 May 1999 "DoD Public Key Infrastructure" memorandum released by the Deputy Secretary of Defense (DEPSECDEF) contained a requirement that the Department of Defense (DoD) Public Key Infrastructure (PKI) policy be reviewed on an annual basis to ensure that the policy remains consistent with evolving technology and DoD objectives. In recent months, the DoD PKI Program Management Office (PMO) and the Military Departments have reviewed the policy and developed recommended changes to some of the DoD PKI timelines and milestones contained in the original 6 May 1999 memorandum. A primary driver for these changes is the direction contained in the 10 November 1999 "Smart Card Adoption and Implementation" memorandum issued by DEPSECDEF, to merge and synchronize DoD PKI implementation efforts with the DoD Common Access Card (CAC) deployment. The DoD PKI PMO worked closely with the DoD CAC stakeholders, primarily the DoD Access Card Office (ACO) and representatives from the Military Departments, to develop the proposed changes to the DoD PKI timelines and milestones.

On 28 April 2000, the DoD PKI PMO briefed the proposed DoD PKI policy changes to the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)). ASD(C3I) concurred with the proposed changes, and issued an updated DoD PKI policy, with new timelines and completion milestones, on 12 August 2000. This Department of the Navy (DON) PKI Implementation Plan is consistent with these new timelines and completion milestones.

Executive Summary

Public Key Infrastructure (PKI) is the keystone for the protection of Department of Defense (DoD) information and is an enabling technology that will enhance information systems security and promote secure electronic business and electronic commerce. Public key cryptography offers the best available technology for secure transmission of unclassified data across public and private wide area networks. It provides a high degree of assurance of data confidentiality, integrity, access control, and user identification among users of networked applications, including e-mail, web-based information services and transactions, and electronic commerce. PKI refers to the framework and services that provide for the secure generation, production, distribution, control, and accounting of public key certificates.

This PKI Implementation Plan for the Department of the Navy (DON) provides a roadmap for Navy and Marine Corps planners and managers to carry out the DoD PKI policy and addresses the general activities and objectives associated with implementation of the Navy and Marine Corps portions of the Class 3, Class 4 (FORTEZZA), and Target Class 4 DoD PKIs. This implementation plan is consistent with the 6 May 1999 "DoD Public Key Infrastructure" memorandum released by the Deputy Secretary of Defense, as modified by the DoD Chief Information Officer (CIO) on 12 August 2000, as well as the 29 October 1999 DoD PKI Implementation Plan. Chief of Naval Operations (CNO) N643 and Headquarters, Marine Corps (HQMC) C4 will promulgate detailed implementation guidance within their respective chains-of-command as necessary to accomplish the specific activities and achieve the specific objectives outlined in this plan.

The long-term DoD goal is to evolve from the current Class 3 and Class 4 DoD PKIs to a single, Target Class 4 DoD PKI offering a higher level of assurance. As standards and technology evolve, today's medium assurance, software-based certificates, hardware-based certificates on tokens and the specialized high assurance solution (i.e., FORTEZZA) will be replaced with universal high assurance certificates and tokens. Hardware tokens, such as smart cards, promise other multiple uses that offer convenience and ease of use in a multitude of information applications. The convergence of these technologies affords the opportunity to provide all DoD computer users with confidentiality, integrity, authentication, and non-repudiation for electronic communications and transactions. DON plans to accelerate implementation of smart card-based tokens by synchronizing, to the greatest extent possible, the Class 3 DoD PKI implementation, DoD Common Access Card (CAC) rollout, and deployment of the Navy Marine Corps Intranet (NMCI). This will provide for increased security over Class 3 software certificates, ensuring the transition to cost-effective, web-enabled, and secure information management solutions throughout DON. Subsequent migrations to higher levels of assurance and more future-generation smart cards will be transparent to end users. Currently issued certificates will not be obviated by the transition from Class 3 to Class 4 certificates, and existing certificates will remain viable for the duration of their expected life cycle. Just as higher speed processors and increased memory are incorporated into routine technology refresh plans for personal computers, smart card capabilities and future enhancements to the assurance level of the DoD PKI will be incorporated seamlessly over time.

The DON PKI implementation strategy requires rapidly fielding a PKI infrastructure together with a public key (PK)-enabled cyber environment (i.e., the NMCI) that supports these converging technologies and enables users to take advantage of these application services as they evolve.

Table of Contents

Foreword ii

Executive Summary iii

1. Introduction 1–1

2. Class 3 DoD PKI Implementation Activities 2–1
   - 2.1 Introduction 2–1
   - 2.2 DON Support To DoD PKI PMO 2–2
   - 2.3 Class 3 Infrastructure Implementation 2–2
     - 2.3.1 Integrated RAPIDS-LRA Workstation Deployment 2–3
     - 2.3.2 LRA Deployment Via NMCI 2–3
     - 2.3.3 Establishment of Additional LRAs 2–3
     - 2.3.4 Operations, Maintenance, and Life Cycle Support 2–4
   - 2.4 Class 3 Certificate Issuance 2–4
   - 2.5 PK-Enabled Application Development and Testing 2–4
   - 2.6 Transition Strategy 2–5
   - 2.7 Implementation of Class 3 PKI on SIPRNET 2–5

3. Class 4 DoD PKI Implementation Activities 3–1
   - 3.1 Introduction 3–1
   - 3.2 DON Support To DoD PKI PMO 3–1
   - 3.3 Class 4 Infrastructure Component Implementation 3–1
     - 3.3.1 Component Acquisition, Installation, and Accreditation 3–2
     - 3.3.2 Operations, Maintenance, and Life Cycle Support 3–2

4. Target Class 4 DoD PKI Implementation Activities 4–1
   - 4.1 Introduction 4–1
   - 4.2 DON Support to DoD PKI PMO 4–1
   - 4.3 Target Class 4 Infrastructure Component Implementation 4–1
     - 4.3.1 Component Acquisition, Installation, and Accreditation 4–2
     - 4.3.2 Operations, Maintenance, and Life Cycle Support 4–2
   - 4.4 PK-Enabled Application Development and Testing 4–2
   - 4.5 Transition Strategy 4–2

Appendix A References A-1

Appendix B Acronym List B-1

1. Introduction

Public key cryptography, using digital certificates, offers the best available technology for secure transmission of unclassified data across public and private wide area networks. Public Key Infrastructure (PKI) refers to the framework and services necessary to generate, issue, and manage public key certificates. These certificates support critical Department of Defense (DoD) applications by providing confidentiality and authentication of network transactions, data integrity, and non-repudiation. This Public Key Infrastructure Implementation Plan for the Department of the Navy (DON) presents the Navy and Marine Corps plan for implementing the PKI policy set forth in the 6 May 1999 Deputy Secretary of Defense (DEPSECDEF) memorandum entitled "Department of Defense Public Key Infrastructure," as modified by the DoD Chief Information Officer (CIO) on 12 August 2000. Figure 1-1 illustrates the top-level timelines and milestones for the DoD PKI.[1]

Milestone Event	Date
All private web servers issued Class 3 certificates	12/31/00
All private web servers perform server-side authentication	12/31/00
Class 3 registration infrastructure deployment complete	12/31/01
Entire target population issued Class 3 certificates	10/31/02
All private web servers require client-side authentication	10/31/02
All e-mail signed appropriately	10/31/02
All networks enabled for hardware token certificate-based access control	10/31/02
Infrastructure upgraded to Target Class 4	10/31/02
Begin issuance of Target Class 4 certificates	10/31/02
All unclassified mission critical systems on unencrypted networks migrate to Target Class 4 certificates/tokens	12/31/03
Discontinue issuance of Class 3 software certificates	10/31/02
Discontinue issuance of Class 3 hardware certificates	12/31/04

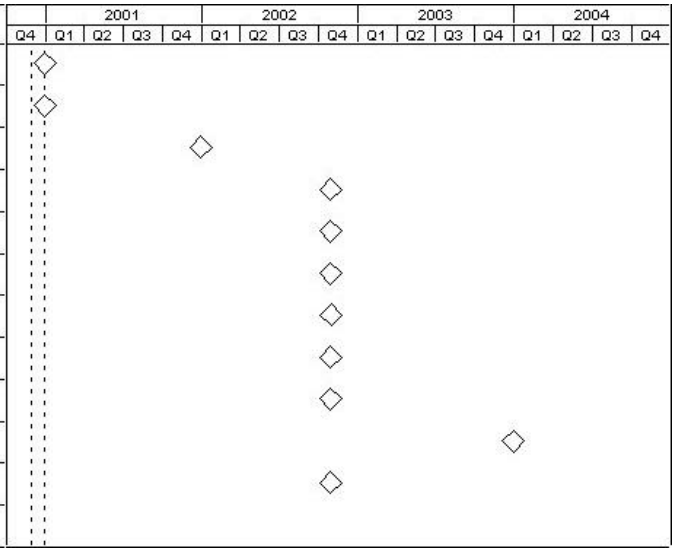

Figure 1-1. DoD PKI Top-Level Timelines and Milestones

The Department of the Navy's Chief Information Officer is responsible for Information Assurance and PKI policy across our enterprise. The principal Navy and Marine Corps organizations responsible for the successful implementation of the DON portion of the DoD PKI are the Office of the Chief of Naval Operations (CNO) N643 and Headquarters Marine Corps (HQMC) C4, respectively. This DON PKI Implementation Plan builds on the DoD PKI Implementation Plan by translating the actions and responsibilities assigned in the DoD plan into specific activities for the Navy and Marine Corps. Based on this DON PKI implementation plan, CNO N643 and HQMC C4 will establish comprehensive PKI implementation programs and/or promulgate detailed PKI implementation guidance within their respective chains-of-command to the extent required to accomplish the activities and achieve the objectives described in this plan.

[1] *Readers unfamiliar with the DoD PKI initiative and the capabilities provided by the DoD PKI should review the Public Key Infrastructure Roadmap for the Department of Defense, dated 29 October 1999, and the Public Key Infrastructure Implementation Plan for the Department of Defense, dated 29 October 1999, both currently available at http://infosec.navy.mil.*

The next 3 sections of this plan address the Navy and Marine Corps implementation activities associated with the Class 3 DoD PKI, Class 4 DoD PKI, and Target Class 4 DoD PKI, respectively. There are two appendices to this document. Appendix A provides a list of references and Appendix B provides an acronym list.

2. Class 3 DoD PKI Implementation Activities

This section defines the general Department of the Navy activities and responsibilities associated with implementation of the DON portion of the Class 3 DoD PKI.

2.1 Introduction

The Class 3 DoD PKI service, which evolved from the DoD Medium Assurance Pilot PKI service, supports the protection of business transactions and sensitive but unclassified (SBU) administrative information. The Class 3 DoD PKI service can also be used on closed networks to provide additional protection such as user authentication, data separation, and support for communities of interest (COI). One example of a closed network where a Class 3 DoD PKI will be implemented is the Secret Internet Protocol Router Network (SIPRNET).

The Class 3 DoD PKI service employs a hierarchical architecture consisting of a centralized Root Certificate Authority (CA) with a single level of subordinate CAs, a small number of Registration Authorities (RA), and a larger number of Local Registration Authorities (LRA). The Class 3 Root CA is currently located at the National Security Agency (NSA) facility in Finksburg, MD, and the Class 3 CAs are currently located at DoD Regional Support Activities (RSA) in Chambersburg, PA, and Denver, CO.

Class 3 RAs are located at selected Service and Agency commands. The Navy RA is currently located at the Director, Communications Security (COMSEC) Material System (DCMS) Headquarters and the primary Marine Corps RA is currently located at the Marine Corps Information Technology Network Operations Center (MITNOC). Both the Navy and Marine Corps may establish additional RAs to support regional and tactical requirements.

Currently, Class 3 LRAs are being established as required at selected Navy and Marine Corps commands, based on initial requirements for Class 3 certificates in the field. Deployment of the Navy Marine Corps Intranet (NMCI), beginning in the first quarter of fiscal year 2001 (Q1FY2001), will generate a large requirement for Class 3 certificates within the DON. The NMCI contractor will establish and operate additional Class 3 LRAs as needed to support the NMCI rollout. Class 3 certificates will not be issued on floppy disks within the DON unless required to meet near-term operational requirements.

Additionally, beginning in January 2001, the Class 3 LRA functionality will be available at DoD Real-time Automated Personnel Identification System (RAPIDS) stations, and Class 3 certificates will be issued on the DoD Common Access Card (CAC)[2], the replacement for the current military identification (ID) card and existing smart cards. A key objective for the DON is to have hardware-based Class 3 certificates on DoD CACs issued to all DON users by October 2002.

Class 3 PKI implementation activities for the DON include:

- Support to the DoD PKI PMO;

[2] *Readers unfamiliar with the DoD CAC initiative and the capabilities provided by the CAC should review the CAC Execution Plan, dated May 2000.*

- Implementation of the Class 3 infrastructure within the Navy and Marine Corps;
- Issuance of Class 3 certificates on CACs to every active duty, selected reserve, government civilian, and on site contractor of the Navy and Marine Corps by the end of FY 2002;
- Development and deployment of public key (PK)-enabled applications;
- Transition of existing medium assurance PKIs (i.e., PKIs that do not comply with Class 3 DoD PKI requirements) to the Class 3 DoD PKI; and
- Implementation of Class 3 PKI on SIPRNET.

2.2 DON Support To DoD PKI PMO

The DoD PKI PMO is responsible for all aspects of Class 3 DoD PKI component and system development and testing. DON participation in these activities generally includes technical document reviews and specific actions assigned by the DoD PKI PMO through the three DoD PKI working groups:

- The **DoD PKI Technical Working Group (TWG)** is responsible for identifying, addressing, and resolving technical and operational issues associated with the implementation and operation of the DoD PKI.
- The **DoD PKI Business Working Group (BWG)** is responsible for addressing DoD PKI business requirements.
- The **DoD PKI Certificate Policy Management Working Group (CPMWG)** is responsible for preparing and coordinating the DoD Certificate Policy (CP), including the creation, review, and update of relevant documentation.

Active DON representation and participation in these working groups is essential to ensuring that all Navy and Marine Corps Class 3 PKI requirements are addressed, correctly interpreted, and properly implemented by the DoD PKI PMO.

2.3 Class 3 Infrastructure Implementation

The DoD PKI PMO is procuring all hardware and software required for implementation of the Class 3 DoD PKI at the Root and CA levels, including all hardware and software required for the Class 3 DoD PKI directories. The DON is responsible for acquiring, installing, accrediting, operating, and maintaining Class 3 RAs, LRAs, and regional/local directory components as required to implement its portion of the Class 3 DoD PKI. Most of the core infrastructure components associated with the Class 3 PKI (i.e., RAs, some directory components and some LRAs) are already in place within the Navy, and are scheduled to be in place by December 2000 in the Marine Corps.

Efforts remaining for the Navy and Marine Corps include coordinating the establishment of Class 3 LRA functional capability at the DoD RAPIDS stations; overseeing the establishment and operation of Class 3 LRAs, and issuance of CACs and Smart Card readers, via NMCI and DEERS/RAPIDS; establishing additional LRAs beyond those provided by DoD RAPIDS stations and the NMCI; and providing Class 3 RA/LRA operations, maintenance, and life cycle support.

2.3.1 Integrated RAPIDS-LRA Workstation Deployment

Beginning in January 2001, the Defense Manpower Data Center (DMDC) will deploy integrated RAPIDS-LRA workstations at approximately 1,200 DoD RAPIDS stations at various locations worldwide. These integrated RAPIDS-LRA workstations will support the issuance of Class 3 identity and e-mail certificates on the DoD CAC to all DoD military (Active Duty and Reserves), civilian, and selected contractor personnel. The deployment of the DoD PKI LRA functionality at the DoD RAPIDS stations (also referred to as the Verification Officer/Local Registration Authority (VO/LRA)) may result in a reduction in the total number of Navy and Marine Corps LRAs that would otherwise be needed.

The Navy and Marine Corps will participate in RAPIDS-LRA implementation planning meetings and forums; periodically review RAPIDS-LRA workstation installation schedules and progress of actual installations; and adjust the overall Navy and Marine Corps LRA installation plans and schedules as appropriate.

2.3.2 LRA Deployment Via NMCI

The NMCI contract will provide the DON with a single, robust and secure corporate intranet and all associated information technology (IT) services, operated and maintained by the NMCI contractor. The NMCI will deploy Smart Card readers to end users and will require Class 3 DoD PKI certificates to access NMCI services and resources. The NMCI contractor will establish and operate LRAs as required for temporary Smart Card tokens (i.e., to support the issuance of certificates to NMCI users who have not yet received their certificates on a DoD CAC). Additionally, the NMCI LRAs will perform other certificate management functions (e.g., revocation requests, limited user troubleshooting, audit data collection, etc.).

The Navy and Marine Corps will participate in NMCI LRA installation planning meetings; periodically review NMCI LRA workstation installation schedules and progress of actual installations; register NMCI LRAs; and adjust the overall Navy and Marine Corps LRA installation plans and schedules as appropriate.

2.3.3 Establishment of Additional LRAs

Establishment of Navy and Marine Corps LRAs will continue as required to support the demand for Class 3 certificates within the DON. Navy commands requiring public key certificates within their respective areas of responsibility prior to establishment of an LRA at the nearest RAPIDS station, or prior to LRA availability via the NMCI, are responsible for establishing, accrediting, operating, and maintaining their own LRAs. LRA establishment and accreditation must be in accordance with DCMS procedures and DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)." Marine Corps commands requiring public key certificates prior to the establishment of an LRA at the nearest RAPIDS station will coordinate their requirements with the Marine Corps RA (MITNOC). Prospective Navy LRAs can obtain technical assistance through the Space and Naval Warfare Systems Command (SPAWARSYSCOM (PMW-161)) customer support function

while Marine Corps LRAs can obtain technical assistance through the MITNOC (See section 2.5 below).

2.3.4 Operations, Maintenance, and Life Cycle Support

Release 2.0 of the Class 3 DoD PKI became operational in July 2000. DCMS is responsible for operating and maintaining the Navy RA(s); MITNOC is responsible for operating and maintaining the primary Marine Corps RA and secondary (regional) RAs; and the individual Navy and Marine Corps commands (or, if applicable, the NMCI contractor) at which LRAs and regional/local directory components are located are responsible for operating and maintaining their respective components. Component maintenance includes maintenance of hardware and operating system software only; Class 3 DoD PKI RA/LRA software upgrades will be maintained and distributed under configuration control procedures established by the DoD PKI PMO.

Standard Operating Procedures (SOP) for LRAs and "Subscriber" PKI instructions for end users are available from the Navy and Marine Corps RAs. Additionally, mandatory formal training for LRAs is available through the DCMS Advice and Assist (A&A) teams for the Navy and through the MITNOC for the Marine Corps. Local and regional help desk support for Navy LRAs and end users is available through the Navy Information Systems Security (INFOSEC) help desk (http://infosec.navy.mil), and similar support is available for Marine Corps LRAs through the regional Marine Corps help desks. As more PKI-aware applications become available, commands will train local Help Desk personnel to address integration issues for end users.

2.4 Class 3 Certificate Issuance

By October 2002, all active duty military personnel, members of the Selected Reserve, DoD civilian employees, and eligible contractor personnel who have access to Navy and Marine Corps Automated Information Systems will have received his or her Class 3 PKI certificate on a DoD CAC. Service members will receive their CACs via the DoD RAPIDS-LRA stations. Although DMDC will install the upgraded integrated RAPIDS-LRA workstation at the DoD RAPIDS stations, the responsibility for issuing DoD CACs remains with the DoD organizations operating the RAPIDS stations. For the Navy and Marine Corps, the DoD RAPIDS stations will typically be located at local Personnel Support Detachment (PSD), Pass & ID, or Security offices. The Navy and Marine Corps must develop specific plans and identify any additional resources needed to support Class 3 certificate and CAC issuance.

2.5 PK-Enabled Application Development and Testing

Where applications employing public key technology are required, the local Navy and Marine Corps application-owning commands are responsible for developing and deploying PK-enabled applications (or integrating commercially available PK-enabled products) that are compatible and compliant with the Class 3 DoD PKI. In accordance with DEPSECDEF memorandum dated 12 August 2000, the migration of PK-enabled applications to DoD Class 3 PKI compliance must begin immediately. By December 2000, all private Navy and Marine Corps web servers must be PK-enabled to perform server-side authentication using Secure

Socket Layer (SSL) Authentication (or better) and DoD Class 3 public key certificates. By October 2002, these private web servers must additionally perform client-side authentication using DoD Class 3 certificates. At the present time, there is no mandate for application-owning commands to PK-enable non-Web-based applications that do not otherwise employ public key technology. However, application-owning commands are encouraged to PK-enable their applications, where there is a sufficient business case to do so.

PMW-161 and MARCORSYSCOM are testing commercially available PK-enabled applications and products (e.g., e-mail applications, web servers, and virtual private networks [VPNs]) and evaluating commercially available PK-enabling toolkits and utilities for the Navy and Marine Corps. Additionally, PMW-161 and the MITNOC have established customer support functions to provide technical assistance to their respective Navy and Marine Corps systems commands, program offices, and local commands responsible for deploying PK-enabled applications and products within their respective areas of responsibility. Additional information about the PK-enabled applications/products test program and customer support function is available through the Navy INFOSEC and MITNOC web sites.

2.6 Transition Strategy

All Navy and Marine Corps PKI pilots and operational PKI implementations that currently exist must transition to the DoD PKI. Public key certificates issued under the current DoD Medium Assurance Pilot PKI need only be replaced with Class 3 DoD PKI certificates on an as-needed basis (e.g., due to loss or compromise of an individual's private key, expiration of the original certificates, or as needed to support PK-enabled applications that only support Class 3), unless it is determined that continued support for certificates issued under the current DoD Medium Assurance Pilot PKI would be overly cumbersome for Navy and Marine Corps Class 3 RAs and LRAs.

2.7 Implementation of Class 3 PKI on SIPRNET

The planned SIPRNET PKI will be implemented as a separate instance of the DoD Class 3 PKI to provide data separation, message integrity, and non-repudiation within a closed network and will not utilize the CAC token. The Department of the Navy will coordinate specific SIPRNET Class 3 PKI implementation actions with the DoD PKI PMO.

3. Class 4 DoD PKI Implementation Activities

This section defines the general Navy and Marine Corps activities and responsibilities associated with implementation of the DON portion of the Class 4 DoD PKI.

3.1 Introduction

The current Class 4 DoD PKI is a FORTEZZA-based service designed primarily to support the Defense Messaging System (DMS). The Class 4 DoD PKI employs a hierarchical architecture. The Root CAs are located at NSA, while the subordinate CAs are located at Navy and Marine Corps base, post, and command sites. At the discretion of local commands, the Class 4 DoD PKI service may be used to support other applications that process unclassified mission critical information. The Class 4 FORTEZZA-based PKI can also be used on closed networks and over networks secured using NSA Type 1 encryption to provide additional protection such as user authentication, data separation, and support for COIs.

The DON has reduced the number of Certificate Authority Workstation (CAW) locations originally planned by regionalizing the CAs at Navy and Marine Corps DMS Area Control Centers (ACC), Local Control Centers (LCC), and Remote Server Sites (RSS). A Navy Central CAW Facility (NCCF) has been established at the COMSEC Material Issuing Office (CMIO) Norfolk. Additional CAs have been authorized at other selected locations. DCMS has been designated as the Class 4 Approval Authority for the Navy and the Marine Corps Systems Command (MARCORSYSCOM) has been designated as the Approval Authority for the Marine Corps.

Class 4 DoD PKI implementation activities for the DON include:

- Support to the DoD PKI PMO; and
- Implementation of the upgraded Class 4 infrastructure components within the Department of the Navy.

3.2 DON Support To DoD PKI PMO

The DMS program office and the DoD PKI PMO are responsible for component/system development and testing activities associated with DMS and the Class 4 DoD PKI. DON participation in these activities generally includes technical document reviews and specific actions assigned by the DoD PKI PMO through the three DoD PKI working groups (DoD PKI TWG, BWG, and CPMWG). Active DON representation and participation in these working groups is essential to ensuring that all DON Class 4 PKI and FORTEZZA requirements continue to be addressed, correctly interpreted, and properly implemented by the DoD PKI PMO.

3.3 Class 4 Infrastructure Component Implementation

The DoD DMS PMO is providing CAW upgrades for the Version 3.1 CAWs originally provided by DISA. DON Class 4 infrastructure component implementation responsibilities include acquiring, installing, and accrediting Class 4 CAW components; and providing operations, maintenance, and life cycle support.

3.3.1 Component Acquisition, Installation, and Accreditation

To support the DON portions of the Class 4 DoD PKI, PMW-161 is coordinating the deployment of CAW Version 4.2.1 hardware and software, at all DON locations beginning in the first quarter of FY 2001. These upgraded workstations will be able to issue both Version 1 and Version 3 X.509 certificates. MARCORSYSCOM is providing inputs to PMW-161 for quantities and locations of CAWs for Marine Corps commands. Local Navy and Marine Corps commands will accredit their CAW and local directory site installations in accordance with the DMS Certification and Accreditation Plan and DoD Instruction 5200.40 (DITSCAP). To assist local commands in the accreditation process, PMW-161 is performing a Security Test and Evaluation (ST&E) at each site at which a Version 4.2.1 CAW upgrade is installed. Additional technical support for sites accrediting their CAW installations is available through PMW-161.

3.3.2 Operations, Maintenance, and Life Cycle Support

Local Navy and Marine Corps commands are responsible for operating and maintaining their Version 3.1 and Version 4.2.1 CAWs. Life cycle support for CAW hardware will be provided by PMW-161, and support for CAW software will be provided by the DoD PKI PMO, as coordinated by PMW-161.

DON CAs, System Administrators (SAs), and Information Systems Security Officers (ISSOs) currently receive formal classroom training on the Version 3.1 CAW through the Army and Air Force training commands. There are currently no plans to integrate formal CA/SA/ISSO training into the Navy training commands or the Marine Corps training infrastructure; DON use of the Army and Air Force facilities is expected to continue for the Version 4.2.1 CAW; training locations are also being established by the Army in Korea and Germany and by the Navy in Hawaii. Additionally, the DoD PKI PMO is developing and plans to provide computer-based training (CBT) for CAW personnel and PKI Instructions for end users. Once approved, the Navy and Marine Corps Approval Authorities will distribute these training products to all commands at which Version 4.2.1 CAWs are installed.

The Navy and Marine Corps will continue to provide local and regional help desk support for CAs and end users through their existing INFOSEC help desks.

4. Target Class 4 DoD PKI Implementation Activities

This section introduces the Target Class 4 DoD PKI and defines the anticipated DON activities and responsibilities associated with implementation of the DON portion of the Target Class 4 DoD PKI, to the extent that these activities and responsibilities are known at this time.

4.1 Introduction

The Target Class 4 DoD PKI will leverage the efforts of both the Class 3 and FORTEZZA-based Class 4 PKI and migrate them to the Target Class 4 DoD PKI. The goal for DoD and the DON is to move as quickly as possible toward the Target Class 4 DoD PKI by establishing the capability to issue hardware-based certificates immediately. To facilitate this migration, the DoD PKI strategy is designed to leverage the capabilities and services offered by the commercial PKI industry. The Target Class 4 DoD PKI will provide an integrated PKI that supports a broad range of security-enabled applications, and provides for secure interoperability within DoD and its federal, allied, and commercial partners while minimizing costs and impact to operations. It will support multiple assurance levels to enable users to cost effectively and efficiently select appropriate security solutions based on the sensitivity or value of the data, the level of risk, and the security of the certificate management information.

Efforts are presently underway to define the Target Class 4 DoD PKI architecture, requirements, implementation strategy, and transition approach (i.e., how DoD will transition the current Class 3 and Class 4 PKIs to the Target Class 4 PKI). Based on preliminary information available from the DoD PKI PMO, Target Class 4 DoD PKI implementation activities for the DON will likely include:

- Support to the DoD PKI PMO;
- Implementation of the Target Class 4 PKI infrastructure components within the DON;
- Development and deployment of Target Class 4 PK-enabled applications; and
- The transition of Class 3 and Class 4 PKI infrastructure components and PK-enabled applications to the Target Class 4 DoD PKI.

4.2 DON Support to DoD PKI PMO

The DoD PKI PMO is responsible for Target Class 4 DoD PKI architecture definition; requirements specification; and component/system acquisition, development, and testing. DON participation in these activities will likely include technical document reviews and specific actions assigned by the DoD PKI PMO through the three DoD PKI working groups (DoD PKI Technical Working Group, Business Working Group, and CPMWG) and the Target Class 4 DoD PKI User Requirements Forum. Active DON representation and participation in these working groups is essential to ensuring that all DON Target Class 4 PKI requirements are addressed, correctly interpreted, and properly implemented by the DoD PKI PMO.

4.3 Target Class 4 Infrastructure Component Implementation

The DoD PKI PMO will procure and deploy the Root, CA, and directory components needed to implement the Target Class 4 DoD PKI. DON Target Class 4 DoD PKI component

implementation responsibilities include acquiring, installing, and accrediting the Target Class 4 DoD PKI RAs, LRAs, local/regional directories, and hardware tokens/readers; and providing operations, maintenance, and life cycle support.

4.3.1 Component Acquisition, Installation, and Accreditation

DoD PKI PMO will conduct a PKI technology and services security assessment, develop an acquisition plan, and procure the PKI and directory components needed to implement the Target Class 4 DoD PKI. The Target Class 4 DoD PKI Root and CA components are scheduled to be deployed by the end of FY 2002. The DON will need to procure and deploy all RA, LRA, and regional/local directory hardware and software needed for implementation of the DON portion of the Target Class 4 DoD PKI. Local certification and accreditation of the Navy and Marine Corps RAs, LRAs, and directories will be performed by local commands in accordance with DoD Instruction 5200.40 (DITSCAP).

4.3.2 Operations, Maintenance, and Life Cycle Support

The anticipated initial operational date for the Target Class 4 DoD PKI is October 2002. Navy and Marine Corps unit commands will be responsible for operating the RAs, LRAs, and local directories, beginning in October 2002. Navy unit commands will also provide life cycle support for RA, LRA, and local directory hardware items. MARCORSYSCOM will provide life cycle support for Marine Corps RA, LRA, and local directory hardware items.

The DoD PKI PMO will develop appropriate formal training material for Target Class 4 DoD PKI RAs, LRAs, and local directory operations, and updated PKI Instructions for end users. The Navy and Marine Corps will be responsible for training their respective LRAs and local directory support personnel. Additionally, the Navy and Marine Corps will provide local and regional help desk support for their LRAs and end users through their INFOSEC help desks.

4.4 PK-Enabled Application Development and Testing

Where applications employing public key technology are required, the local Navy and Marine Corps application-owning commands are responsible for developing and deploying PK-enabled applications (or integrating commercially available PK-enabled products) that are compatible and compliant with the Target Class 4 DoD PKI. As with Class 3 PK-enabled applications, application-owning commands are encouraged to PK-enable their applications to comply with Target Class 4 PKI requirements, where there is a sufficient business case to do so.

The respective PMW-161 and MITNOC PK-enabled applications/products test programs and customer support functions established to support the Class 3 PKI will be upgraded as necessary to provide similar support for Target Class 4 DoD PKI-compliant applications and products.

4.5 Transition Strategy

The DON will participate in the development of the transition strategy plan for the Target Class 4 DoD PKI to the extent that the transition strategy plan is staffed for review and comment

by the DoD PKI PMO through the DoD PKI Working Groups. It is anticipated that the DON will need to migrate their Class 3 and Class 4 PKI components (i.e., CAs and any regional and local directories) to the respective Target Class 4 DoD PKI platforms in accordance with the overall Target Class 4 DoD PKI transition strategy. Similarly, DON Class 3 and Class 4 PK-enabled applications may need to be modified or upgraded to be brought into compliance with Target Class 4 DoD PKI interface requirements. By 31 December 2003, when public key cryptography is used for protection of Mission Critical information on unclassified networks, Target Class 4 certificates must be used, however, Class 3 certificates may be issued through December 2004 and be supported until natural expiration. Subsequent migrations to higher levels of assurance and more future-generation smart cards will be transparent to end users. Currently issued certificates will not be obviated by the transition from Class 3 to Class 4 certificates, and existing certificates will remain viable for the duration of their expected life cycle. Just as higher speed processors and increased memory are incorporated into routine technology refresh plans for personal computers, smart card capabilities and future enhancements to the assurance level of the DoD PKI will be incorporated seamlessly over time.

Appendix A
References

1. Assistant Secretary of Defense (C3I) Memorandum, "Department of Defense (DoD) Public Key Infrastructure (PKI)," 12 August 2000

2. Department of Defense Access Card Office, "CAC Execution Plan (Draft)," May 2000

3. Chief of Naval Operations (N6) Message NAVADMIN 110/00, "Navy Public Key Infrastructure (PKI) Implementation," 011504Z MAY 00

4. United States Department of Defense X.509 Certificate Policy, Version 5.0, 13 December 1999

5. Deputy Secretary of Defense Memorandum, "Smart Card Adoption and Implementation," 10 November 1999

6. Department of Defense, "Public Key Infrastructure Roadmap for the Department of Defense, Version 3.0," 29 October 1999

7. Department of Defense, "Public Key Infrastructure Implementation Plan for the Department of Defense, Version 2.0," 29 October 1999

8. Department of the Navy Chief Information Officer Memorandum, "Department of the Navy Public Key Infrastructure (PKI) Implementation," 21 June 1999

9. Deputy Secretary of Defense Memorandum, "Department of Defense (DoD) Public Key Infrastructure," 6 May 1999

10. OASD (C3I), Department of Defense (DoD) Memorandum- Assignment of Program Management Office Responsibilities for the Department of Defense Public Key Infrastructure, 9 April 1999

11. Department of Defense Instruction 5200.40, Defense Information Technology Security Certification and Accreditation Process (DITSCAP), 30 December 1997

Appendix B
Acronym List

A&A	Advice and Assist
ACC	Area Control Center
ACO	Access Card Office
ASD(C3I)	Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
CA	Certificate Authority
CAC	Common Access Card
CAW	Certificate Authority Workstation
CBT	Computer-Based Training
CINC	Commander in Chief
CIO	Chief Information Officer
CMIO	COMSEC Material Issuing Office
CNO	Chief of Naval Operations
COI	Community of Interest
COMSEC	Communications Security
CP	Certificate Policy
CPMWG	Certificate Policy Management Working Group
C/S/A	CINC, Service, and Agency
DCMS	Director, COMSEC Material System
DEPSECDEF	Deputy Secretary of Defense
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DMDC	Defense Manpower Data Center
DMS	Defense Messaging System
DoD	Department of Defense
DON	Department of the Navy
FY	Fiscal Year
HQMC	Headquarters, Marine Corps
ID	Identification
INFOSEC	Information Systems Security
ISSO	Information System Security Officer

IT	Information Technology
LCC	Local Control Center
LRA	Local Registration Authority
MARCORSYSCOM	Marine Corps Systems Command
MITNOC	Marine Corps Information Technology Network Operations Center
NCCF	Navy Central CAW Facility
NMCI	Navy Marine Corps Intranet
NSA	National Security Agency
PK	Public Key
PKI	Public Key Infrastructure
PMO	Program Management Office
PSD	Personnel Support Detachment
Q	Quarter
RA	Registration Authority
RAPIDS	Real-time Automated Personnel Identification System
RSA	Regional Support Activity
RSS	Remote Server Site
SA	System Administrator
SBU	Sensitive But Unclassified
SIPRNET	Secret Internet Protocol Router Network
SOP	Standard Operating Procedure
SPAWARSYSCOM	Space and Naval Warfare Systems Command
ST&E	Security Test and Evaluation
VO	Verification Officer
VPN	Virtual Private Network